Dr. Gerrit Hornung, LL.M.
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Universität Kassel

Regelungsinstrumente im virtuellen Raum

Vortrag bei Sommerakademie 2010 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD): „Codex digitalis. Optimierter Persönlichkeitsschutz – digital und vernetzt“

Kiel, 30. August 2010

1. Das Thema meines Vortrags bewegt sich schon im Ausgangspunkt des Titels in einem Spannungsverhältnis: Der Begriff der „Regelung“ oder des „Regelungsinstruments“ entstammt erkennbar einer nationalstaatlichen Perspektive, die im Grundsatz von der Regelungsbedürftigkeit, vor allem aber von der Regelungsfähigkeit eines Problems, und damit von der Durchsetzungsmacht der regulierenden Instanz ausgeht. Der „virtuelle Raum“ des Internets hingegen ist aus rechtlicher Perspektive – weitere, hochspannende Blickwinkel wie die der Philosophie, Soziologie, Psychologie und andere lasse ich hier weg – vor allem durch drei Merkmale charakterisiert: Globalität, Intransparenz und Unkörperlichkeit.

2. Die Globalität des Internets führt dazu, dass im „virtuellen“ Raum zwar reale Menschen mit anderen realen Menschen kommunizieren, dabei vor realen technischen Endgeräten sitzen, die mit realen Netzwerken verbunden sind, und häufig reales Geld bezahlen (und mitunter reale Schäden erleiden) – diese Prozesse aber grenzüberschreitend und weltweit ablaufen. Die damit verbundenen Probleme der Bestimmung des anwendbaren nationalen Rechts und seines Inhalts überfordert nicht nur, aber jedenfalls den durchschnittlichen Nutzer des Netzes.

Unter anderem daraus folgt das zweite Charakteristikum, die fehlende Transparenz. Diese hat aber noch weitere Gründe: Die technisch überbrückte Distanz erzeugt Informationsgefälle, in denen die Nutzer häufig über ihre Kommunikationspartner, die verantwortlichen Stellen und die bewirkten Datenverarbeitungsprozesse im Unklaren bleiben. Drittens ist der virtuelle Raum dadurch gekennzeichnet, dass er keinen körperlichen Rahmen, keine physische Zeit, keine körperlichen Sachen und keine körperlichen Akteure zu haben scheint. Das hat vielfältige Folgen für die Rechtsordnung. Für die hier hergebrachten Regelungsinstrumente hat es – zusammen mit der Globalität – vor allem ein Vollzugsdefizits zur Folge. Nationalstaatliche Institutionen können häufig der Verantwortlichen nicht habhaft werden, um das anwendbare Recht durchzusetzen. Kann man die Akteure identifizieren, sind auf einen Sachverhalt häufig andere Rechtsordnungen anwendbar, in denen bestimmte, aus der eigenen Rechtsordnung wohlbekannte rechtliche Schutzmechanismen fehlen – die Grundprinzipien des deutschen und europäischen Datenschutzrechts sind hierfür ein gutes Beispiel.

Die durch die drei Merkmale der Globalität, Intransparenz und Unkörperlichkeit verursachten Probleme aktualisieren und verstärken sich insbesondere dort, wo global organisierte Unternehmen mit möglicherweise sogar monopolartigen Wettbewerbspositionen im virtuellen Raum auftreten – darauf wird zurückzukommen sein.

Aus der nationalstaatlichen Perspektive ist bei allen Problemen meines Erachtens offensichtlich, dass das Regelungsbedürfnis bestehen bleibt oder sogar größer wird. Der virtuelle Raum hat nicht weniger Regelungsprobleme, nicht weniger Regelungsbedarf. Verfassungsrechtlich folgt dies bereits aus den grundrechtlichen Schutzpflichten des Staates. Die alten nationalstaatlichen Instrumente für nationale, transparente und körperliche Verhältnisse sind aber auf

die neuen Probleme der Globalität, der Intransparenz und der Unkörperlichkeit nicht übertragbar. Damit stellt sich die Frage: Was wirkt im virtuellen Raum?

3. Zur Beantwortung der Frage ist im Ausgangspunkt die Unterscheidung zwischen staatlichen und privaten Akteuren wichtig. Wenn und soweit der Staat im Internet als Akteur auftritt, können datenschutzrechtliche Fragen eben doch weithin aus nationalstaatlicher Perspektive behandelt werden. Das betrifft zum einen die Regulierung des E-Governments, also aktuell etwa Identitätsinfrastrukturen, die der (deutsche) Staat entweder selbst betreibt oder für die er starke Vorgaben machen kann. Zum anderen sind aber auch die sicherheitsrechtlichen Ermächtigungsgrundlagen – und ihre rechtsstaatlichen Begrenzungen –, die für das Internet normiert werden, „Regelungsinstrumente im virtuellen Raum". Das Bundesverfassungsgericht hat hier in den letzten Jahren eine Fülle von Vorgaben gemacht, die bei weitem noch nicht ausdiskutiert oder gar umgesetzt sind, aber weithin unter Anwendung hergebrachter Regulierungsinstrumente auf nationaler oder europäische Ebene behandelt werden können.

Unter dem Gesichtspunkt der Regulierungsproblematik sind dagegen die privaten Kommunikations- und Interaktionspartner der Internetnutzer viel wichtiger (und interessanter). Ich werde mich deshalb im Folgenden auf diesen Bereich beschränken.

4. Regulierung in diesem Bereich bedeutet zunächst, diesen Begriff weit zu verstehen: Regulierung muss nichts mit dem Staat zu tun haben, nichts mit Gesetzen, nichts mit konditional aufgebauten Ge- oder Verbotsnormen. Schon die Einladung zur Veranstaltung nennt ja sehr zu Recht: „Betriebsvereinbarungen, Codes of Conduct, Verträge, Schutzziele, Standards für Technik und Organisation; angesichts der globalen gesellschaftlichen Herausforderungen sind die Gesetzgeber gefordert, aber nicht nur diese."

5. Da der Gesetzgeber also nicht allein, wohl aber auch gefordert ist, gestatten Sie mir zwei Bemerkungen zur Reform des Datenschutzrechts, die heute ja in mehreren anderen Vorträgen Gegenstand war und sein wird.

Zum einen ist aus meiner Sicht überdeutlich, dass eine rein nationale Regulierung des „virtuellen Raums" in Zeiten internationaler Anbieter- und Kundenverflechtungen weder wünschenswert noch möglich ist. Wenn wir also über die Modernisierung des Datenschutzrechts sprechen, müssen wir – zumindest auch – über die Modernisierung des europäischen Datenschutzrechts sprechen. Die Datenschutzrichtlinie für die elektronische Kommunikation ist Ende letzten Jahres in einigen Punkten aktualisiert worden, aber die allgemeine europäische Datenschutzrichtlinie stammt aus dem Jahre 1995. Fünfzehn Jahre sind in der Entwicklung des Internets eine Ewigkeit (können Sie sich noch vorstellen, wie das Internet im Jahre 1995 aussah? – es hatte jedenfalls wenig bis nichts mit dem „virtuellen Raum" zu tun, um den es hier geht). Die in der Richtlinie verbürgten Grundsätze sind aber noch erheblich älter. Der Bedarf nach einer adäquaten Regulierung für das Internetzeitalter besteht insbesondere auf einer europäischen, besser noch über Europa hinausreichenden Eben, weil nur so das Risiko einer Flucht in Rechtsordnungen vermindert werden kann, deren Datenschutzniveau aus deutscher Perspektive ungenügend ist.

Der europäische Modernisierungsbedarf ist erheblich – er steht aber genau deshalb auch in erheblichem Maße nationalen Modernisierungsbestrebungen entgegen. Dieser Aspekt ist meines Erachtens in der aktuellen Diskussion noch zu wenig beleuchtet worden. Zwar gab es schon vor zehn Jahren im Zusammenhang mit der Debatte um das Modernisierungsgutachten hierzu Erörterungen in der Wissenschaft. Welche politische Sprengkraft die Frage haben könnte, lässt sich aber etwa an der Diskussion um die Abschaffung des Listenprivilegs ablesen, in der die Werbewirtschaft die Richtlinienwidrigkeit des Entwurfs behauptete. Inwieweit die Richtlinie Regelungsspielräume bietet und wieweit ihre Harmonisierungswirkung reicht, ist umstritten – das entbindet aber nicht davon, nationale Modernisierungsideen an diesem Maßstab zu prüfen. Das Eckpunktepapier der Konferenz der Datenschutzbeauftragten vom

18. März dieses Jahres – das viele gute und wichtige Hinweise enthält – blendet diesen Gesichtspunkt etwa vollständig aus.

Ein zweiter Gesichtspunkt zur Reform des Datenschutzrechts: Das das Modernisierungsgutachten im Auftrag des BMI ist inzwischen fast zehn Jahre alt, der Reformbedarf ist seit vielen Jahren allgemeine Meinung, und er ist Gegenstand mehrerer Koalitionsvereinbarungen auf Bundesebene gewesen. Da dies alles dennoch nicht zu einer umfassenden Reform geführt hat, sollte zumindest erwogen werden, Alternativen zur Strategie einer umfassenden Neuordnung zu finden. Prof. Roßnagel hat hierzu unlängst die Idee eines „Musterentwurfs“ vorgebracht, um einen Maßstab dafür zu gewinnen, ob einzelne kleinere Reformschritte in die „richtige“ Richtung gehen oder nicht. Ich glaube, dass diese Idee viel für sich hat.

6. Damit möchte ich das Recht in seiner herkömmlichen Form und Funktion hinter mir lassen, und mich alternativen Regulierungsstrategien zuwenden. Die bereits erwähnte „zweite Generation“ von Regelungsinstrumenten wird – mit mehr oder weniger expliziten Bezügen zur generellen Steuerungsdebatte – seit deutlich über zehn Jahren diskutiert und ist insoweit keineswegs im eigentlichen Sinn „neu“. Ohne Anspruch auf Vollständigkeit zählen zu der zweiten Generation: die staatliche Förderung des Selbstdatenschutzes, der den Betroffenen technische Mittel zum Schutz ihrer Privatsphäre an die Hand gibt; der Systemdatenschutz, also rechtliche und wirtschaftliche Anreize für eine möglichst datenschutzfreundliche, insbesondere datenvermeidende und datensparsame Gestaltung von Datenverarbeitungssystemen; Konzepte der Selbstregulierung (Codes of Conduct, Standardvertragsklauseln, Best Practices und andere), die für eine stärkere Selbstverpflichtung der Unternehmen sorgen; Datenschutz-Audits und Gütesiegel, die eine höhere Transparenz für die Betroffenen und einen Wettbewerb um datenschutzfreundliche Technologien ermöglichen. Gerade das ULD ist beim Datenschutz-Audit und Datenschutz-Gütesiegel ja erfreulicher Vorreiter der Entwicklung.

Konzeptionell fehlt es also nicht an Instrumenten; wohl aber fehlt es nach wie vor an der breiten Umsetzung und Anwendung auf die virtuellen Räume (nicht nur) des Internets. Nicht jedes dieser Instrumente wird dabei in jeder Situation und für alle Beteiligten das richtige sein. In ihrer Gesamtheit geben sie aber die richtigen Antworten auf die Entstehung virtueller Räume und den durch diese verursachten neuen Regelungsbedarf, weil sie rechtliche Instrumente durch technische Schutzmechanismen ergänzen, flexibler und schneller wirken als die mitunter schwerfällige Gesetzgebung und die wirtschaftlichen Eigeninteressen der Beteiligten für die Erreichung der Regulierungsziele mobilisieren. Sie zielen damit auf die Charakteristika des virtuellen Raums, die eingangs erläutert wurden. Sie zielen überdies auf die Umsetzung „softer“ datenschutzrechtlicher Vorgaben und sind deshalb für das Thema von doppelter Bedeutung. „Weiche“ Vorgaben wie das Gebot der Datenvermeidung und Datensparsamkeit sind mit ordnungsrechtlichen Vorgaben kaum operationalisierbar, sondern nur, wenn verantwortliche Stellen und Hersteller für eine aktive Mitwirkung gewonnen werden können. Dies wiederum setzt voraus, dass diese für sich selbst Vorteile erkennen. Diese zutreffende Überlegung steht insbesondere hinter Audit- und Gütesiegelkonzepten. Umso bedauerlicher ist es, dass das lang angekündigte Ausführungsgesetz zum Datenschutzaudit auf Bundesebene im letzten Jahr gescheitert ist.

Im Übrigen gäbe es zu den einzelnen Instrumenten je nach beteiligten Institutionen und betroffenen Interessen, anwendbarem Recht und Anwendungskontext viel zu sagen. Ich muss und möchte mich hier auf einige übergreifende Gedanken beschränken.

7. Zunächst handelt es sich bei vielen dieser Instrumente um so genannte hybride Regelungsmodelle. Hybrid insoweit, als den handelnden privaten Akteuren ein mehr oder weniger großer Spielraum gegeben wird, der Staat aber bestimmte Mindeststandards garantiert. Das gilt etwa im Bereich der regulierten Selbstregulierung, Codes of Conduct, Vorgaben für Schutzziele, Technik und Organisation etc. Hybride Regelungsmodelle beinhalten insoweit eine

staatliche Letztverantwortung – und setzen damit die prinzipielle Handlungsfähigkeit des Staates voraussetzen. Damit wenden sich allerdings die Zweifel an dieser Handlungsfähigkeit, die im virtuellen Raum prinzipiell bestehen, im Kern auch gegen hybride Modelle. Das spricht nicht prinzipiell gegen diese Strategien, wohl aber aus diesem Blickwinkel und mit Blick in die Zukunft.

An dieser Überlegung wird deutlich – so die These –, dass Regelungsinstrumente, einschließlich der genannten Regelungsinstrumente der „2. Generation" dann effektiv sind, wenn sie über eine Form von „Anker" verfügen. Diese Anker sollten zumindest teilweise die drei anfangs erläuterten Merkmale des virtuellen Raums kompensieren: Wenn dieser durch Globalität, Intransparenz und Unkörperlichkeit gekennzeichnet ist, so sollten Anker national/europäisch, transparent und körperlich sein. Mit anderen Worten ist zur Vermeidung von Vollzugsdefiziten beides erforderlich: intelligente neue Regelungsinstrumente, und deren Verankerung.

Diese Anker können unterschiedlich aussehen. Es kann sich erstens um materiell-rechtliche Vorgaben für die Datenverwendung, die Gestaltung von Datenverarbeitungssystemen, die Formulierung von Codes of Conduct oder Standardvertragsklauseln handeln – so die Möglichkeit der Durchsetzung der Vorgaben besteht. Der Anker kann zweitens auch mehr auf der verfahrenstechnischen Ebene liegen, nämlich hauptsächlich in den rechtlichen oder faktischen Zugriffsmöglichkeiten auf Betreiber und Infrastrukturen, daneben auch in der Beteiligung an und Beeinflussung von technischen Standardisierungsverfahren. Ein politischer Anker kann drittens in einem entsprechenden Skandalisierungspotential liegen. Schließlich kommen viertens wirtschaftliche Anker in Betracht, wenn der Staat oder ein Staatenverbund wie die Europäische Union über entsprechende hinreichende Einflussmöglichkeiten verfügt.

8. Diese vier Typen von „Ankern" sind natürlich nicht untereinander austauschbar, können sich aber durchaus teilweise kompensieren. Ein Beispiel dafür ist die aktuelle Diskussion um Google Streetview. Ohne diese rechtlich zu bewerten, scheint es mir doch so zu sein, dass der Anker der materiellen Schranken des Datenschutzrechts erheblich weniger deutlich ist als die Zugriffsmöglichkeiten, die durch das Erfordernis der Datenerhebung vor Ort mittels Kameras eröffnet wurden sowie die faktische Zuordnung durch den Sitz von Google Germany in Hamburg – und sicher weniger wichtig als der Anker der öffentlichen Meinung, der offenbar ein erhebliches politisches Potential inne hatte und hat.

Umgekehrt ist erkennbar, dass hergebrachte und moderne Regelungsinstrumente ohne Anker wenig effektiv sind. Das gilt etwa für die Entwicklung datenschutzfreundlicher Technik und ihren Einsatz in der Praxis. Nehmen Sie das Beispiel der so genannten Location Based Services: Zum Thema ihrer datenschutzfreundlichen Gestaltung sind allein in unserem Institut in den letzen Jahren drei Dissertationen entstanden. Das Wissen für einen Datenschutz durch Technik ist also verfügbar, in der Praxis ändert aber etwa ein Konzern wie Apple seine AGB für sämtliche Plattformen des IT-Konzerns und lässt sich das Recht einräumen, die Positionsdaten der Nutzer zu speichern und an Partner weiterzugeben – über etwaige Anonymisierungstechniken herrscht weiterhin Unklarheit. Ein zweites Beispiel ist das automatische Scannen von E-Mails durch Googles E-Mail Dienst Gmail, um personalisierte Werbung zu ermöglichen – eine inhaltliche Analyse, die mit dem einfachgesetzlichen Fernmeldegeheimnis des § 88 Abs. 3 TKG nicht vereinbar ist, aber auf der Basis der Datenschutzerklärung von Google geschieht.

Wiederum ohne diese Vorgehensweisen im Detail auf ihre Zulässigkeit zu prüfen, könnte es sein, dass derartige Player wie Apple, Google oder Facebook die maßgeblichen Akteure bei der Formulierung des – globalen – Codex Digitalis sein werden, über den wir heute sprechen. Das gilt auch für neue Anwendungen wie das Cloud Computing: Hier setzen Anbieter wie Amazon und Google technische Standards, deren datenschutzrechtliche Probleme erst in An-

sätzen erfasst sind, jedenfalls aber kaum dazu führen werden, dass Infrastrukturentscheidungen nachträglich revidiert werden. Vielleicht bilden also diese Global Player die neuen Regeln, so wie dies historisch im Fall der lex mercatoria, also dem im Mittelalter entstandenen Gewohnheitsrecht der Handelsleute, der Fall war? Könnte ein derartiges Gewohnheitsrecht des virtuellen Raums wichtiger sein als nationale Bestrebungen – schlicht und einfach deswegen, weil sich globale Marktmacht mit hunderten von Millionen Nutzern selbst ihre Regeln gibt?

Ich gestehe, dass ich für diese grundsätzlich skeptische Perspektive – leider – zumindest in den Bereichen Anlass sehe, in denen globale Konzerne Geschäftsmodelle finden und diese sich zumindest einigen der genannten Anker entziehen. Ich will abschließend dennoch einige Punkte aufzeigen, an denen man gegenüber globalen Playern ansetzen könnte.

9. Wenn es stimmt, dass auf diesem Wege Regulierung stattfindet, dann muss es darum gehen, diese Akteure, ihre Organisation und Entscheidungsprozesse so zu stimulieren, dass diese den Persönlichkeitsschutz der Menschen berücksichtigen. Eine Konzentration auf die Global Player, die das Gewohnheitsrecht des Internets mitgestalten können, erscheint dabei durchaus angemessen: Wenn Organisationen wie Apple und Google datenschutzfreundlich handeln würden, wäre so viel im virtuellen Raum abgedeckt, dass nicht nur für die einzelnen Betroffenen sehr viel gewonnen wäre, sondern auch Leitbildfunktionen entstehen könnten. Gewendet auf die Ausgangsfrage der Regulierung gerade im virtuellen Raum bedeutet dies, nicht so sehr neue Regulierungsinstrumente für diesen zu erfinden – diese sind vielmehr zumindest konzeptionell verfügbar –, sondern vielfältige und kräftige Anker für diese Instrumente zu entwickeln.

Was also könnten Mittel hierfür sein? Erstens kann der regulierende Staat dort auf Augenhöhe auftreten, wo er selbst mit wirtschaftlicher Macht auftritt oder die Ausübung privater wirtschaftlicher Macht zu regulieren vermag – also im Bereich rechtlicher Vorgaben für die Beschaffung von Datenverarbeitungssystemen durch den Staat selbst (Beschränkung auf datenschutzfreundlich zertifizierte Systeme) oder durch Private (Anreize oder Verpflichtung zu entsprechender Beschaffung). Zweitens eröffnen sich Einflussmöglichkeiten durch das Setzen von Standards dort, wo der Staat ausnahmsweise schneller ist oder sein könnte als die private Wirtschaft. Ein Beispiel könnte – noch wissen wir nicht, ob es so kommen wird – die Authentisierung mittels des elektronischen Identitätsnachweises des elektronischen Personalausweises sein. Werden derartige hoheitlich betriebene oder garantierte Infrastrukturen datenschutzfreundlich betrieben (aber auch nur dann), besteht die Chance datenschutzfreundlicher Spillover-Effekte auch bei Global Players.

Drittens sehe ich Ansätze für diese großen Anbieter bei einer Übertragung von Regulierungsansätzen aus dem Bereich des Kartellrechts. Die Markt- und Rechtsmacht der Europäischen Union hat es hier immerhin geschafft, Microsoft eine Entkoppelung von Betriebssystem und Internet Explorer abzutrotzen. Offenbar bestehen entsprechende Möglichkeiten, wenn Europa in einem bestimmten Bereich gewillt ist, zum Schutz seiner Bürger entsprechende Konflikte in Kauf zu nehmen. Wo ein solcher Wille fehlt, sollte in Zukunft verstärkt daran erinnert werden, dass grundrechtliche Schutzpflichten nicht nur den deutschen, sondern auch den europäischen Gesetzgeber binden. In Übernahme kartellrechtlicher Ansätze könnte man für Unternehmen oder Dienste mit erheblicher Marktmacht zumindest eine Pflicht zur Bereitstellung von Schnittstellen für datenschutzfreundliche Anbieter andenken (etwa im Fall Google vs. Scroogle).

Viertens sollten schließlich informelle Prozesse einer Regulierung durch Herstellung politischer Öffentlichkeit nicht unterschätzt werden. Dieser Anker mag auf den ersten Blick leichtgewichtig sein, aus juristischer Perspektive misstrauisch beäugt werden oder Anlass für (in Teilen berechtigte) Kritik an der Qualität politischer Debatten sein. Er könnte aber zumindest

dort wirksam werden, wo mehrere Faktoren zusammen kommen: Eine Öffentlichkeit, die hinreichend für Datenschutzfragen sensibilisiert ist, ein politischer Raum, der so groß ist, dass auch multinationale Unternehmen ihn nicht einfach übergehen können, und Institutionen, die gewillt und in der Lage sind, entsprechende Prozesse informeller Regulierung zu initiieren. Hierin wird meines Erachtens – weiterhin – eine nicht unerhebliche Bedeutung der künftigen Arbeit des ULD und seiner Mitstreiter liegen und liegen müssen.

10. Was schließlich die Leitbilder der Bildung dieser oder anderer Anker angeht, so sind diese mannigfaltig diskutiert. Es geht um die Förderung von Transparenz (etwa durch Informationspflichten der Anbieter: nicht notwendig mehr, aber deutlichere), um die Stärkung von Betroffenenrechten, um Privacy by Default (Einschränkungen sind begründungspflichtig: das gilt sowohl für staatliche Eingriffe wie für die Grundeinstellungen in sozialen Netzwerken), auch um die Ernstnahme der Nutzer und ihrer Bedürfnisse – unter Einschluss der Bedürfnisse nach Kommunikation über soziale Netzwerke, die anders aussehen können als die Bedürfnisse in der Offline-Welt. Letztlich geht es um den Schutz des digitalen Bürgers und seiner Identität.

Wenn wir unter derartigen Leitbildern Anker für die Regulierung schaffen, solle es möglich sein, Einfluss auf Infrastrukturen zu nehmen, die heute gestaltet, morgen implementiert und übermorgen genutzt werden. Wenn das gelingt, bin ich auch zuversichtlich, dass die realen Persönlichkeitsrechte im virtuellen Raum angemessen geschützt werden können.